6. Custom Scan: Because even network security likes its coffee made a certain way!

A `Custom Scan` is a targeted method used in network security to evaluate specific vulnerabilities or areas within a network. It enables cybersecurity experts to focus on particular segments, ports, or protocols, optimizing resources and identifying critical weaknesses more effectively.

The security team decides to use an advanced `Nmap` scan that manipulates `TCP flags` to create non-standard packets, which are typically not used in regular communications but might be utilized by attackers to probe and exploit vulnerabilities in network defenses.

Write a bash script that executes a `custom scan`. The script should configure Nmap to send packets with all possible `TCP flags` set, targeting ports `80` to `90` on a specified host.

- Your script should accept `host` as an arguments `$1`.
- Your script should accept `ports` as an arguments `$2`.
- Your script should save the output to the file `custom_scan.txt`.
- Your script should redirect both error messages and standard output to ensure nothing appears on the screen.

Depending on the scanned network, the output could change.

```
┌──(maroua)-[~/0x06_nmap_advanced_port_scans]
└─🏴‍☠️ ./6-custom_scan.sh www.holbertonschool.com 80-90
[sudo] password for maroua:
┌──(maroua)-[~/0x06_nmap_advanced_port_scans]
└─🏴‍☠️ cat custom_scan.txt
# Nmap 7.80 scan initiated Fri Apr 19 19:30:06 2024 as: nmap -scanflags
URGACKPSHRSTSYNFIN -p 80-90 -oN custom.txt www.holbertonschool.com
Nmap scan report for www.holbertonschool.com (3.233.126.24)
Host is up (0.16s latency).
Other addresses for www.holbertonschool.com (not scanned): 34.234.52.18
52.206.163.162 64:ff9b::34ce:a3a2 64:ff9b::22ea:3412 64:ff9b::3e9:7e18
rDNS record for 3.233.126.24: ec2-3-233-126-24.compute-1.amazonaws.com

PORT   STATE    SERVICE
80/tcp filtered http
81/tcp filtered hosts2-ns
82/tcp filtered xfer
83/tcp filtered mit-ml-dev
```

```
84/tcp filtered ctf
85/tcp filtered mit-ml-dev
86/tcp filtered mfcobol
87/tcp filtered priv-term-l
88/tcp filtered kerberos-sec
89/tcp filtered su-mit-tg
90/tcp filtered dnsix

# Nmap done at Fri Apr 19 19:30:10 2024 -- 1 IP address (1 host up) scanned in 4.55 seconds
```

`sudo nmap --scanflags -p$2 $1 -oN custom_scan.txt >/dev/null 2>&1`

Breakdown

1. **`sudo`**:
   - Runs the `nmap` command with superuser privileges. Some advanced scan options in Nmap require root privileges to execute.
2. **`nmap`**:
   - This is the command-line tool Nmap (Network Mapper), which is used for network discovery and security scanning.
3. **`--scanflags`**:
   - This option allows you to manually set custom TCP flags in the packets Nmap sends. You would normally use this to specify a combination of TCP flags (such as `FIN`, `SYN`, `ACK`, `PSH`, `URG`, and `RST`) to create a specific kind of scan. For example, `--scanflags URGACK` would set both URG and ACK flags.
4. **`-p$2`**:
   - The `-p` flag specifies the port or range of ports you want to scan. In this case, `$2` represents the second argument passed to the script, which should be a specific port or range of ports, such as `80` or `80-90`.
5. **`$1`**:
   - This represents the first argument passed to the script, which should be the target IP address or hostname to scan.
6. **`-oN custom_scan.txt`**:
   - This option directs Nmap to save the scan results in the specified file, `custom_scan.txt`, in a normal (readable) output format.

7. **`>/dev/null 2>&1`**:
    - This part redirects all output (both standard output and standard error) to `/dev/null`, which essentially discards it. `>/dev/null` redirects the standard output, and `2>&1` redirects standard error to the same place, ensuring that nothing appears on the screen.

Example Command with Flags Set

If you wanted to specify TCP flags, you'd add them directly after `--scanflags`. Here's an example of setting **all TCP flags** (like an Xmas scan):

```
sudo nmap --scanflags URGACKPSHRSTFIN -p$2 $1 -oN custom_scan.txt >/dev/null 2>&1
```

Summary

This command will:

- Run an Nmap scan with specified TCP flags on a target host (`$1`) and port range (`$2`).
- Save the scan results to `custom_scan.txt`.
- Discard any screen output, so only the file `custom_scan.txt` will contain the scan results.

This configuration is typically used for stealth scans where you want to avoid alerting anyone monitoring the network.